National Security Agency/Central Support Service

INFORMATION ASSURANCE DIRECTORATE

CGS Network Intrusion Prevention Capability

Version 1.1.1

Network Intrusion Prevention employs a response to perceived anomalous activity on the network. When this activity is perceived, Network Intrusion Prevention encompasses mechanisms to react to block, drop, redirect, and/or quarantine anomalous activities. Network Intrusion Prevention is enabled through network-based modules deployed throughout the network.

07/30/2012

CGS Network Intrusion Prevention Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Network Intrusion Prevention employs a response to perceived anomalous activity on the network. When this activity is perceived, Network Intrusion Prevention encompasses mechanisms to react to block, drop, redirect, and/or quarantine anomalous activities. Network Intrusion Prevention is enabled through network-based modules deployed throughout the network.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

Network Intrusion Prevention is the Capability that provides first line of protection against anomalous activity by responding to signature alerts. It is enabled through a network-based module or appliance rather than a single host. Network Intrusion Prevention devices respond to perceived anomalous activity on a network, as they occur, with little or no human interaction.

The Network Intrusion Prevention Capability is implemented through network-based modules and prevents incidents occurring on the network by reacting to anomalous activity or perceived anomalous activity, as it occurs, on the network to maintain operational integrity and security. Network Intrusion Prevention systems protect networks from the network layer to the application layer, against known and unknown malicious activity. In addition, the Network Intrusion Prevention Capability shall be implemented at layers 3 and higher within the Open System Interconnection (OSI) model, not just on the network layer. Network Intrusion Prevention network-based modules shall be located at the network boundaries, both outside and inside the boundaries (as defined within the Network Boundary and Interfaces Capability), with additional modules placed in front of critical network components.

The Network Intrusion Prevention Capability shall be managed centrally on an out-of-band (OOB) network. Policy shall be configured and pushed from the central management console (policy is defined within the Digital Policy Management Capability, in accordance with the Incident Response/Analysis or Risk Mitigation Capabilities). Communication between Network Intrusion Prevention network modules shall not take place because the network modules are configured and updated through a central manager. Communications between the Capability and the central manager shall occur over secure channels (see the Communication Protection Capability). Security administrators monitor and tune Network Intrusion Prevention mechanisms to minimize false positives and false negatives while allowing execution of prevention activities.

The Network Intrusion Prevention Capability shall use a managed signature repository (as provided by the Signature Repository Capability) to keep its attack signatures up to date. Network Intrusion Prevention shall use Enterprise-predefined policy in responding whenever an anomalous activity is detected. Network Intrusion Prevention shall have the ability to react to Network Intrusion Detection (NID) or other Capability alerts or signatures. A typical response may be to block all traffic from the source Internet Protocol (IP) address, block incoming traffic on that port, and redirect any packets, stopping a process, or blocking malicious system calls from writing to protected directories, to proactively protect the host or network. In addition to an intrusion response, Network Intrusion Prevention also sends an alert notification to the appropriate security administrators within the Enterprise to notify them of the action it has taken against the attack or threatening activity, which is a response or action that is commensurate with policy requirements. Policy shall identify maximum response times in formal incident response procedure guidance.

Alerts sent by Network Intrusion Prevention shall contain source/destination address, time, signature, action taken, and whether the action was a success or failure. Alerts shall be provided using OOB mechanisms and be encrypted (as provided by the Communication Protection Capability). Alerts shall be stored in a centralized, OOB, encrypted repository in accordance with current Enterprise policies and standards. Alerts shall be formatted and provide information in accordance with current industry data standards.

Network Intrusion Prevention shall have policies and rules that prohibit certain types of behavior or activities on the network. In addition, Network Intrusion Prevention can be configured to respond to any traffic that violates the Network Intrusion Prevention rules. These rules shall allow Network Intrusion Prevention to react in near real-time (as it

occurs) to anomalous activities. Depending on the criticality of the protected portion of the network and availability requirements, Network Intrusion Prevention shall implement either failover or redundant solutions.

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. The infrastructure supports the use of an OOB network for centralized management.
2. The Enterprise provides an up-to-date signature repository.
3. Policies exist that define what network and incident response behavior is expected.
4. The infrastructure provides the necessary storage for alerts and backups.
5. The Enterprise will perform investigative actions based on alerts provided.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability reacts to malicious or anomalous activity to prevent attacks.
2. The Capability generates alerts of its actions containing source/destination address, time, signature, action taken, and success or failure.
3. A single network will use diverse Network Intrusion Prevention solutions rather than a single vendor solution.
4. The prevention actions may create a denial of service.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

When the Network Intrusion Prevention Capability is implemented correctly, the Organization will possess a capability to provide an automated response to perceived

anomalous activity on a network, as quickly as policy requires. The ability to respond without human assistance is crucial because anomalous activity may occur at any time. Long-term sustainability of the Network Intrusion Prevention Capability will require human interaction for system maintenance. In addition, administrators will be required to verify that responses mitigate the detected threats. Analysis shall include (1) independent follow-up examination for signs that threats with known signatures and effects succeeded despite the Network Intrusion Prevention response, (2) correlation with Host Intrusion Detection alerts, and (3) examination to discover whether Network Intrusion Prevention response is being used to the attacker's advantage.

An Organization will employ only technologies and products that have been approved by the Organization for use on its networks. An Enterprise will need to be able to write and implement rules for use of products and technologies for its Network Intrusion Prevention Capability, which prohibit certain types of behavior or activities on or by the network. This will be done in accordance with the Organization's risk analysis process and in keeping with the Information Assurance (IA) Policies, Procedures, and Standards Capability.

Network Intrusion Prevention is designed to perform a prevention action, such as block, drop, redirect, or quarantine anomalous activities. Attackers may be able to use these actions to their advantage by causing misconfigurations in the network modules that implement the Network Intrusion Prevention Capability. Therefore these network modules will be centrally managed via OOB mechanisms, which use secure, encrypted communication that incorporates proper authentication between the modules and the central manager that configures them.

The Organization will employ a Network Intrusion Prevention solution that provides centralized management. Centralized management will facilitate Enterprise-wide configuration changes to the Network Intrusion Prevention Capability on all networks from one location. The Organization may need to perform the initial baseline manually to ensure that the configuration does not inhibit the network operations. Other than this instance, central management is structured such that manual configuration will not occur, and the Configuration Management Capability will provide the configurations for distribution to the network-based modules. Individual agencies will determine, based on policy, when individuals are given access to the Network Intrusion Prevention policy on the network to make individual modifications.

The Organization will ensure that Network Intrusion Prevention has its attack signatures kept up to date by a centrally managed signature repository (see Signature Repository

Capability) to stay up to date on the latest threats and how to handle them, because anomalous activities are always evolving, with new exploit techniques and malicious code being written all the time. The Network Intrusion Prevention central management function will be responsible for obtaining the signatures from the Signature Repository, which will provide definitions, patterns, and behaviors of malicious activity for Network Intrusion Prevention. These signatures will then be pushed out from the central manager to the Network Intrusion Prevention agents. These signatures will be used to prevent worms, viruses, Trojans, and spyware and define response actions to be executed by Network Intrusion Prevention.

To determine how the Network Intrusion Prevention Capability will operate on the network, the Organization will use penetration testing. The Organization will determine the Network Intrusion Prevention mechanisms work correctly without impacting the network while using them in a test environment. The test environment itself may not employ Network Intrusion Prevention devices for mission reasons. Once the Network Intrusion Prevention has been tested, the Organization will deploy the approved Network Intrusion Prevention configuration for use on the host.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Network Mapping-The Network Intrusion Prevention Capability relies on the Network Mapping Capability to provide visualization of the network to determine placement of intrusion prevention devices.
- Network Boundary and Interfaces-The Network Intrusion Prevention Capability relies on the Network Boundary and Interfaces Capability to provide information about network boundaries so that malicious activity can be prevented from crossing the Enterprise's network borders.
- Utilization and Performance Management-The Network Intrusion Prevention Capability relies on the Utilization and Performance Management Capability to provide information on dynamic fluctuations, which may identify anomalous activity

(e.g., increase in outbound network traffic may imply data exfiltration; an increase in service requests may imply a denial-of-service attempt).

- Understand Mission Flows-The Network Intrusion Prevention Capability relies on the Understand Mission Flows Capability to identify key resources that fulfill mission objectives. These resources are prioritized when deploying network intrusion prevention systems.
- Network Boundary Protection-The Network Intrusion Prevention Capability relies on the Network Boundary Protection Capability for information used to understand and define the trust relationship between the connecting networks and enclaves to determine whether an intrusion has taken place.
- Signature Repository-The Network Intrusion Prevention Capability relies on the Signature Repository Capability to obtain signatures that define known attack patterns in order to take preventative actions.
- Network Intrusion Detection-The Network Intrusion Prevention Capability relies on the Network Intrusion Detection Capability to identify perceived anomalous activity within a network-based module so that the associated network traffic can be redirected or blocked to prevent intrusions.
- Incident Response-The Network Intrusion Prevention Capability relies on the Incident Response Capability to determine what actions to take in response to perceived incidents.
- Contingency Planning-The Network Intrusion Prevention Capability relies on the Contingency Planning Capability to provide mission disruption and recovery information to inform decision-making processes and the formulation of possible courses of action.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management-The Network Intrusion Prevention Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards-The Network Intrusion Prevention Capability relies on the IA Policies, Procedures, and Standards Capability to provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.
- IA Awareness-The Network Intrusion Prevention Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.

- IA Training-The Network Intrusion Prevention Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities-The Network Intrusion Prevention Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- System Protection-The Network Intrusion Prevention Capability relies on the System Protection Capability to provide the protection measures that are implemented on the intrusion prevention systems to prevent unauthorized access or modification of rules.
- Communication Protection-The Network Intrusion Prevention Capability relies on the Communication Protection Capability to enable the secure transmission of responses, logs, and communications to and from intrusion prevention systems.
- Network Enterprise Monitoring-The Network Intrusion Prevention Capability relies on the Network Enterprise Monitoring Capability to monitor the status of intrusion prevention devices.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
CM-7 *LEAST FUNCTIONALITY*	Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services: [Assignment: organization-defined list of prohibited or restricted functions, ports, protocols, and/or services]. Enhancement/s: (1) The organization reviews the information system

	[Assignment: organization-defined frequency] to identify and eliminate unnecessary functions, ports, protocols, and/or services. (2) The organization employs automated mechanisms to prevent program execution in accordance with [Selection (one or more): list of authorized software programs; list of unauthorized software programs; rules authorizing the terms and conditions of software program usage]. (3) The organization ensures compliance with [Assignment: organization-defined registration requirements for ports, protocols, and services].
SC-26 *HONEYPOTS*	Control: The information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, and analyzing such attacks. Supplemental Guidance: None. Enhancement/s: (1) The information system includes components that proactively seek to identify web-based malicious code.
SI-4 *INFORMATION SYSTEM MONITORING*	Enhancement/s: (3) The organization employs automated tools to integrate intrusion detection tools into access control and flow control mechanisms for rapid response to attacks by enabling reconfiguration of these mechanisms in support of attack isolation and elimination. (5) The information system provides near real-time alerts when the following indications of compromise or potential compromise occur: [Assignment: organization-defined list of compromise indicators]. (6) The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities. (7) The information system notifies [Assignment: organization-defined list of incident response personnel (identified by name and/or by role)] of suspicious events and takes [Assignment: organization-defined list of least-disruptive actions to terminate suspicious events]. (8) The organization protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion. (9) The organization tests/exercises intrusion-monitoring tools

	[Assignment: organization-defined time-period]. (10) The organization makes provisions so that encrypted traffic is visible to information system monitoring tools. (11) The organization analyzes outbound communications traffic at the external boundary of the system (i.e., system perimeter) and, as deemed necessary, at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies. (12) The organization employs automated mechanisms to alert security personnel of the following inappropriate or unusual activities with security implications: [Assignment: organization-defined list of inappropriate or unusual activities that trigger alerts].
SI-11 *ERROR HANDLING*	Control: The information system: a. Identifies potentially security-relevant error conditions; b. Generates error messages that provide information necessary for corrective actions without revealing [Assignment: organization-defined sensitive or potentially harmful information] in error logs and administrative messages that could be exploited by adversaries; and c. Reveals error messages only to authorized personnel. Enhancement/s: None Applicable

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Network Intrusion Prevention Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified.

Initiative [CNCI]), 8 January 2008, Classified	Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDI 8410.02 NetOps for the Global Information Grid (GIG), 19 December 2008, Unclassified	Summary: This instruction established DoD policy: c. Global Information Grid (GIG) Enterprise Management (GEM), GIG Net Assurance (GNA), and GIG Content Management (GCM) functions shall be operationally and technically integrated to ensure simultaneous and effective monitoring, management, and security of the enterprise. d. As information systems capabilities mature, they shall be capable of reporting their system status to include fault, configuration, performance, and security to facilitate GIG health and mission readiness assessments. In the section for Responsibilities of Assistant Secretary of Defense for Networks and Information Integration (ASD(NII))/DoD Chief Information Officer (CIO): e. Develop NetOps capability increments in collaboration with functional owners and Capability Portfolio Managers to ensure efficient and secure GIG operations.
DoDI 8420.01, Commercial Wireless Local Area Network (WLAN) Devices, Systems, and Technologies, 3 November 2009, Unclassified	Summary: This instruction establishes policy, assigns responsibilities, and provides procedures for the use of commercial wireless local area network (WLAN) devices, systems, and technologies to achieve and increase joint interoperability; appropriately protect Department of Defense (DoD) information; and enhance overall security to sufficiently protect DoD information by embracing open standards for WLAN devices, systems, and technologies. It provides guidance on establishing a wireless network intrusion detection capability for monitoring local area networks (LANs).
DoDD 8500.01E, Information Assurance (IA), 23 April 2007, Unclassified	Summary: This directive establishes policy and assigns responsibilities to achieve DoD information assurance (IA) through a Defense-in-Depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution to network-centric warfare. It includes policy that DoD information systems shall be monitored based on the assigned mission assurance category and

	assessed risk to detect, isolate, and react to intrusions, disruption of services, or other incidents that threaten the IA of DoD operations or information technology (IT) resources, including internal misuse. DoD information systems also shall be subject to active penetrations and other forms of testing used to complement monitoring activities in accordance with DoD and component policy and restrictions.
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense (CND), 12 August 2008, Unclassified	Summary: This instruction provides joint policy and guidance for IA and Computer Network Defense (CND) operations. It includes policy that DoD information systems (e.g., enclaves, applications, outsourced IT-based process, and platform IT interconnections) will be monitored based on the assigned Mission Assurance Category (MAC), confidentiality level (CL), and assessed risk to detect, isolate, and react to incidents, intrusions, disruption of services, or other unauthorized activities (including insider threat) that threaten the security of DoD operations or IT resources, including internal misuse. In addition, it established policy that the interconnection of information systems will be managed continuously to minimize Community risk and employ protection procedures to restrict access and isolate network segments. Intrusion prevention systems are one device capable of performing this security function.
DISA Enclave Security Technical Implementation Guide (STIG), version 4.2, 10 March 2008, Unclassified	Summary: This Security Technical Implementation Guide (STIG) provides Organizations an overview of the applicable policy and additional STIG documents required to implement secure information systems and networks while ensuring interoperability. Minimum enclave requirements to secure the enclave boundary and the information systems that reside within include external network intrusion detection system, anomaly detection, or prevention device; and internal network intrusion detection system.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	

Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Network Intrusion Prevention Standards

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Department of Defense, Computer Network Defense (CND), Enterprise Sensor Grid (ESG), Strategic Plan, Version 1.0, 9 December 2005, Classified	Summary: This document provides guidance on the usage of network intrusion prevention.
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
NIST SP 800-36, Guide to Selecting Information Technology Security Products, October 2003, Unclassified	Summary: This special publication (SP) describes the characteristics of several categories of IT security products and seeks to help Organizations make informed decisions when selecting IT security products. The categories of products listed include operational controls such as intrusion detection and prevention for both hosts and networks.
NIST SP 800-48, Guide to	Summary: This SP provides guidance to Organizations in

Securing Legacy IEEE 802.11 Wireless Networks, July 2008, Unclassified	securing their legacy Institute of Electrical and Electronics Engineers (IEEE) 802.11 WLAN that cannot use IEEE 802.11i. A wireless intrusion detection and prevention system (WIDPS) is an effective tool for determining whether unauthorized users or devices are attempting to access, have already accessed, or have compromised a WLAN.
NIST SP 800-61 Rev 1, Computer Security Incident Handling Guide, March 2008, Unclassified	Summary: This SP provides practical guidelines on establishing an effective incident response program and responding to incidents effectively and efficiently. Its primary focus is detecting, analyzing, prioritizing, and handling incidents. Continually monitoring threats through intrusion detection and prevention systems (IDPSs) and other mechanisms is essential. Configuring network and host intrusion detection (HID) software to identify activity associated with infections is among the actions to be performed when containing a malicious code incident.
NIST SP 800-83, Guide to Malware Incident Prevention and Handling, November 2005, Unclassified	Summary: This SP provides recommendations for improving an Organization's malware incident prevention measures and gives extensive recommendations for enhancing existing incident response capability so that it is better prepared to handle malware incidents, particularly widespread ones. Organizations should have a robust incident response process capability that addresses malware incident handling. As part of their threat mitigation effort, Organizations should perform threat mitigation to detect and stop malware before it can affect its targets. Intrusion prevention systems are one tool to assist in this effort.
NIST SP 800-94, Guide to Intrusion Detection and Prevention Systems (IDPS), February 2007, Unclassified	Summary: This SP describes the characteristics of IDPS technologies and provides recommendations for designing, implementing, configuring, securing, monitoring, and maintaining them. The types of IDPS technologies are differentiated primarily by the types of events that they monitor and the ways in which they are deployed. The guide provides practical, real-world guidance for each of four classes of IDPS products: network-based, wireless, network behavior analysis, and host-based.

Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	
Other Standards Bodies (ISO, ANSI, IEEE, …)	
Nothing found	

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Scope–The number of boundaries to monitor, the amount of traffic, and the size of network all affect how much work this Capability will have to do.
2. Availability requirements–There is the possibility that the prevention system could lock out authorized systems or data unintentionally. This could violate system availability requirements and mission objectives and require additional time and manpower to fix.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Network Intrusion Prevention Capability.

- The Enterprise shall employ the use of network intrusion prevention systems on the network to respond to perceived anomalous activity as it occurs with little or no human interaction.
- Network intrusion prevention modules shall protect the network from the network layer to the application layer.
- Network intrusion prevention modules shall protect the network against known and unknown malicious activity.
- Network intrusion prevention modules shall be located at the network boundaries, both inside and outside of the boundary.
- Network intrusion prevention modules shall be placed in front of critical network components.
- Network intrusion prevention modules are managed centrally on an OOB network.
- Policy updates shall be pushed to the network intrusion prevention modules from the centralized management system.
- Communication between network intrusion prevention modules shall occur only when the centralized management console acts as an intermediary.
- Communications between the centralized management system and the network intrusion prevention modules shall occur over secure channels.
- Security administrators shall monitor and tune network intrusion prevention mechanisms to minimize false positives and false negatives while allowing execution of prevention activities.
- Network intrusion prevention modules shall use a managed signature repository to keep its attack signatures up to date.
- Network intrusion prevention modules shall use Enterprise-defined policy in responding whenever anomalous activity is detected.
- Network intrusion prevention modules shall have the ability to respond to alerts or signatures produced by other systems.
- The network intrusion prevention system shall send alert notifications to the appropriate security administrators within the Enterprise to notify them of the action it has taken against the attack or threatening activity.
- The Enterprise shall establish policy to identify maximum response times.

- Alerts sent by the network intrusion prevention system shall contain source/destination address, time, signature, action taken, and whether the action was a success or failure.
- Alerts sent by the network intrusion prevention system shall be provided using OOB mechanisms and be encrypted.
- Alerts sent by the network intrusion prevention system shall be stored in a centralized, OOB, encrypted repository in accordance with current Enterprise policies and standards.
- Alerts sent by the network intrusion prevention system shall be formatted and provide information in accordance with current industry data standards.
- The network intrusion prevention system shall use policies and rules to prohibit certain types of behavior or activities on the network.
- The Enterprise shall implement failover or redundant solutions, as necessary, for the network intrusion prevention system.